AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1.   (Currently Amended) A method, comprising:
generating by a first apparatus which controls access to a radio communications network a shared secret at the first apparatus and storing the shared secret in a memory of the first apparatus, wherein the stored secret is associated with an operational mode of the first apparatus where a user of the first apparatus is not to be interrupted and where the stored secret is used for automatic pairing when the first apparatus is in the operational mode;

making the stored shared secret available at a second apparatus;

receiving a signal from the second apparatus to establish communication initiate a pairing process with the first apparatus on the radio communications network, where the signal comprises a request to pair with the first apparatus for a required service from the first apparatus;

determining whether the first apparatus is in the operational mode where [[a]] the user of the first apparatus does not want is not to be interrupted and whether the required service is associated with the stored shared secret; and

for the case where it is determined that the first apparatus is in the operational mode where the user of the first apparatus does not want is not to be interrupted and the required service is associated with the stored shared secret, then creating a secret key for use in pairing to secure communication between them, where the

~~secret key is created using an algorithm~~ <u>initiating the automatic pairing, with no</u>

<u>intervention from the user of the first apparatus, using the stored shared secret</u> or

else

prompting the user of the first apparatus to enter a shared secret associated with the requested

service <u>and initiating the pairing using the user entered shared secret</u>.

2.   (Currently Amended) The method as claimed in claim 1, where the <u>initiated</u>

<u>pairing comprises an</u> algorithm <u>that</u> uses one of the stored shared secret and the

shared secret entered by the user as an input to the algorithm.

3.   (Currently Amended) The method as claimed in claim 1, further comprising, based on

~~at least the created secret key~~ <u>the initiated pairing</u>, establishing the communication with the

second apparatus and providing the requested service to the second apparatus.

4.   (Previously Presented) The method as claimed in claim 1, wherein the determined

operational mode comprises a gaming mode.

5.   (Currently Amended) The method as claimed in claim 1, further comprising, selecting

the operational modes ~~where~~ <u>in which</u> the user of the first apparatus ~~does not want~~ <u>is not</u> to be

interrupted.

6.   (Previously Presented) The method as claimed in claim 1, where the required service

comprises a gaming service.

7.   (Previously Presented) The method as claimed in claim 1, wherein making the stored

shared secret available at the second apparatus involves prompting a user input of the shared

secret at the second apparatus.

8.   (Previously Presented) The method as claimed in claim 1 where the shared secret

comprises a secret PIN.

9.   (Currently Amended) The method as claimed in ~~claim 1~~ claim 2, wherein the algorithm ~~creating~~ creates a secret key for use in the pairing and where the secret key uses a random number communicated between the first apparatus and the second apparatus.

10.   (Currently Amended) The method as claimed in ~~claim 1~~ claim 9, wherein the algorithm creating the secret key uses an identifier of one of the first apparatus and the second apparatus, communicated between the first apparatus and the second apparatus, in the creation of the secret key.

11.   (Previously Presented) The method as claimed in claim 1, further comprising: re-using the stored shared secret to join a third apparatus to the radio communications network without contemporaneous user input of the shared secret at the first apparatus, comprising: making the stored shared secret available at the third apparatus; and

creating in the first apparatus, using the shared secret, a secret key; and making the secret key available to the third apparatus for use in pairing the third apparatus and the first apparatus to secure communication between them.

12.   (Currently Amended) A method, comprising:

storing, in a memory of a second apparatus a shared secret, wherein the stored shared secret is associated with an operational mode of the second apparatus where a user of the second apparatus is not to be interrupted and where the stored secret is used for automatic pairing when the second apparatus is in the operational mode;

sending a signal to a first apparatus to ~~establish communication~~ initiate a pairing process with the first apparatus, where the signal comprises a request to pair with the first apparatus for a required service from the first apparatus;

determining whether the second apparatus is in an operational mode where [[a]] the user of the second apparatus does not want is not to be interrupted and whether the required service is associated with the stored shared secret; and

for the case where it is determined that the second apparatus is in the operational mode where the user of the second apparatus does not want is not to be interrupted and the required service is associated with the stored shared secret, then creating a secret key for use in establishing the communication with the first apparatus, where the secret key is created using an algorithm initiating the automatic pairing, with no intervention from the user of the second apparatus, using the stored shared secret, or else

prompting the user of the second apparatus to enter a shared secret associated with the requested service and initiating the pairing using the user entered shared secret.

13.   (Currently Amended) The method as claimed in claim 12, where the initiated pairing comprises an algorithm that uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm.

14.   (Currently Amended) An apparatus comprising:

a user interface; a memory storing

at least one processor; and

at least one memory including computer readable instructions, where the at least one memory and the computer readable instructions are configured, with the at least one processor, to cause the apparatus to at least:

store a shared secret for use in securing communications in a radio communications network comprising the apparatus and one or more additional apparatus, wherein the stored shared secret is associated with an operational mode of the apparatus where a user of the apparatus is not to be interrupted and where the stored secret is used for automatic pairing when the apparatus is in the operational mode;

a radio transceiver configured to communicate in the network and to receive a signal from the one or more additional apparatus to establish communication initiate pairing with the apparatus on the communications network, where the signal comprises a request to pair with the apparatus for a required service from the apparatus;

at least one processor configured to determine whether the apparatus is in an operational mode where [[a]] the user of the apparatus does not want is not to be interrupted and whether the required service is associated with the stored shared secret; and

the at least one processor configured, for the case where it is determined that the apparatus is in the operational mode where the user of the apparatus does not want is not to be interrupted and the required service is associated with the stored shared secret, to create a secret key for use in pairing the apparatus and the one or more additional apparatus to secure communication between them, where the secret key is created using an algorithm initiate the automatic pairing, with no intervention from the user of the apparatus, using the stored shared secret, or else

the user interface configured to prompt the user of the apparatus to enter a secret associated with the requested service and initiate pairing using the user entered shared secret.

15.   (Currently Amended) The apparatus as claimed in claim 14, where the initiated pairing comprises an algorithm that uses one of the stored secret and the secret entered by the user as an input to the algorithm.

16.   (Previously Presented) The apparatus as claimed in claim 14, wherein the operational mode comprises a game mode.

17.   (Previously Presented) The apparatus as claimed in claim 14, wherein the required service comprises a gaming service.

18.   (Currently Amended) The apparatus as claimed in claim 14, comprising the ~~at least one processor is configured~~ apparatus is caused, in response to the determining, to access the secret in the memory to create ~~the~~ a secret key for use in the pairing without user intervention.

19.   (Currently Amended) The apparatus as claimed in ~~claim 14~~ claim 18, wherein the ~~at least one processor is configured~~ apparatus is caused to automatically create the secret key in response to the received signal.

20.   (Previously Presented) The apparatus as claimed in claim 14, wherein the stored shared secret is independent of an origin of the received signal.

21.   (Currently Amended) The apparatus as claimed in ~~claim 14~~ claim 18, wherein the secret key is dependent upon an origin of the received signal.

22.   (Currently Amended) The apparatus as claimed in ~~claim 14~~ claim 18, wherein the secret key is dependent upon content of the received request.

23.   (Previously Presented) The apparatus as claimed in claim 22, wherein the request includes a random value used with at least the stored shared secret to create the secret key.

24.   (Currently Amended) The apparatus as claimed in claim 14, wherein the ~~at least one processor is configured~~ apparatus is caused, in a first mode, to obtain a secret by accessing the shared secret stored in the memory, ~~is configured,~~ in a second mode, to obtain a shared secret by enabling user input of data, and ~~is configured,~~ in the first mode and in the second mode, to

7

create, using the obtained shared secret, the secret key for use in pairing the apparatus and the one or more additional apparatus to secure communication between them.

25.   (Previously Presented) The apparatus as claimed in claim 24, wherein the first mode is an interactive gaming mode and second mode is an idle mode.

26.   (Currently Amended) The apparatus as claimed in claim 14, wherein the ~~memory stores an apparatus~~ the apparatus is caused to store an apparatus identifier for use with at least the stored shared secret to create the secret key.

27.   (Currently Amended) The apparatus as claimed in claim 15, further comprising the ~~user interface is configured~~ the apparatus is caused to program the value of the stored shared secret.

28.   (Previously Presented) The apparatus as claimed in claim 14, wherein the secret key is for use in securing all communications in the network.

29.   (Currently Amended) The memory embodying instructions executable by a processor of claim 35, where initiating the pairing comprises using an algorithm and where the algorithm uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm.

30.   (Currently Amended) The apparatus as claimed in claim 14, further comprising the ~~user interface is configured to enable data entry, wherein~~ apparatus is caused, when the apparatus participates in a different network controlled by a different apparatus, ~~the user interface is configured~~ to enter a shared secret stored at the different apparatus and ~~the at least one processor is configured~~ to create, using the entered shared secret, a secret key for securing communication.

31-33. (Canceled)

34. (Currently Amended)   An apparatus comprising:

at least one processor; and

at least one memory including computer readable instructions, where the at least one memory and the computer readable instructions are configured, with the at least one processor, to cause the apparatus to at least:

a user interface;

a radio transceiver configured to communication on a radio communications network;

a memory storing store a shared secret for use in securing communications in the radio communications network, wherein the stored shared secret is associated with an operational mode of the apparatus where a user of the apparatus is not to be interrupted and where the stored shared secret is used for automatic pairing when the apparatus is in the operational mode;

the radio transceiver configured to send a signal to another apparatus to establish communication initiate a pairing process with the another apparatus on the communications network, where the signal comprises a request to pair with the another apparatus for a required service from the another apparatus;

at least one processor configured to determine whether the apparatus is in an operational mode where the user of the apparatus does not want is not to be interrupted and whether the required service is associated with the stored shared secret; and

the processor configured, for the case where it is determined that the apparatus is in the operational mode where [[a]] the user of the apparatus does not want is not to

9

be interrupted and the required service is associated with the stored shared secret, ~~to create a secret key for use in pairing over the communications network the~~ ~~apparatus and the another apparatus to secure communication between them, where~~ ~~the secret key is created using an algorithm~~ initiate the automatic pairing, with no intervention from the user of the apparatus, using the stored shared secret, or else

~~the user interface configured to~~ prompt the user of the apparatus to enter a shared secret associated with the requested service and initiate pairing with the another apparatus using the user entered shared secret.

35. (Currently Amended)   A memory embodying a program of computer readable instructions that when executed by a processor perform actions directed to securing communication between a first and second apparatus, the actions comprising:

generating a shared secret at the first apparatus which controls access to a radio communications network and storing the shared secret in a memory of the first apparatus, wherein the stored shared secret is associated with an operational mode of the first apparatus where a user of the first apparatus is not to be interrupted and where the stored shared secret is used for automatic pairing when the first apparatus is in the operational mode;

making the stored shared secret available the second apparatus;

receiving a signal from the second apparatus to ~~establish communication~~ initiate a pairing process with the first apparatus on the radio communications network, where the signal comprises a request to pair with the first apparatus for a required service from the first apparatus;

determining whether the first apparatus is in an operational mode where [[a]] the user of the first apparatus ~~does not want~~ is not to be interrupted and whether the required service is associated with the stored shared secret; and

10

for the case where it is determined that the first apparatus is in the operational mode where the user of the first apparatus ~~does not want~~ is not to be interrupted and the required service is associated with the stored shared secret then ~~creating a secret key for use in establishing the communication with the second apparatus, where the secret key is created using an algorithm~~ initiating the automatic pairing, with no intervention from the user of the first apparatus, using the stored shared secret, or else

prompting the user of the first apparatus to enter a shared secret associated with the requested service and initiate pairing with the second apparatus using the user entered shared secret.

36. (Previously Presented) The memory embodying instructions executable by a processor of claim 35, wherein the operational mode comprises a game mode.

37. (Currently Amended) The apparatus as claimed in claim 34 where initiating the pairing comprises using an algorithm and where the algorithm uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm.